Guidelines for Implementing an

Information Technology Business Continuity Program

for King County Organizations

Organization Information Technology Business Continuity Program Management

1. Establish an organization program based on the King County Information Technology Business Continuity Policy and the following program elements, as appropriate, to support the continuity of essential business services.

- ✓ Enabling authority: King County Information Technology Business Continuity Policy
- ✓ Define organization information technology business continuity directive
- ✓ Define organization information technology business continuity program vision
- ✓ Define organization information technology business continuity program mission
- ✓ Define organization information technology business continuity goals and objectives
- ✓ Define organization information technology business continuity plans and procedures
- ✓ Define organization information technology business continuity regulatory environment
- ✓ Define organization information technology business continuity financial constraints

2. Appoint and authorize the program manager to:

- ✓ Manage the information technology business continuity program
  - to perform the program's administrative functions.
  - to keep the program current and up-to-date by preparing, implementing, evaluating, revising and updating the program, as appropriate.
- ✓ Be the single point of contact as subject matter expert for the organization

3. Establish and evaluate organization information technology business continuity program objectives to support the continuity of essential business services:

- ✓ Establish performance objectives
  - establish management and operational objectives.
- ✓ Evaluate performance objectives on a periodic basis
  - evaluate program management and operational objectives.

4. Participate in King County information technology governance meetings as scheduled.

Core Elements for Organization Information Technology Business Continuity Programs

5. Develop an organization information technology business continuity program to manage information technology business continuity that includes the following minimum elements to support the continuity of essential business services:

- ✓ Inventory essential business services and critical information technology assets that support those services
  - identify essential business services
  - evaluate critical information technology infrastructure
- ✓ Address specific information technology organizational risks that may impact essential business services
  - information technology risk evaluation and control
    - internal and external risk
    - program and project risk
  - information technology business impact analysis
    - internal and external impacts
    - program and project impacts
    - identify interdependencies
- ✓ Implement information technology mitigation strategies
  - prepare gap analysis
  - create information technology mitigation work plans
  - implement information technology mitigation work plans
- ✓ Implement information technology strategic planning process
  - carry out contingency, response, recovery, and resumption processes
- ✓ Implement information technology reviews and training
  - risk mitigation analysis and review
  - contingency plan review
  - training, testing, exercise, lessons learned on program elements

Description of Core Elements with Essential Processes for Organization Information Technology Business Continuity Programs

6. Identify laws and authorities applicable to essential business services that may govern events at all levels

- ✓ Comply with the official expectations that govern the operation of each organization's information technology business continuity program and the King County Information Technology Business Continuity Policy
- ✓ Implement a strategy to review and revise the official expectation that govern the organization's information technology business continuity program and the King County Information Technology Business Continuity Policy
- ✓ Identify other authorities that may be applicable

7. Inventory essential business services and critical information technology assets that support those services

- ✓ identify essential business services
  - map critical information technology assets and processes to essential business services
  - define allowable outage times for critical information technology business processes, functions, and systems including dependent and interdependent software applications
  - prioritize essential business services
  - prioritize business processes

- ✓ evaluate critical information technology infrastructure
  - inventory essential business processes that support essential business services
    - identify interdependencies
  - inventory critical information technology assets that support essential business processes
    - identify interdependencies

8. Perform information technology risk assessment and business impact analysis within the scope of supporting essential business services

- ✓ Perform a information technology risk assessment and during plan updates as appropriate
  - perform an information technology hazard analysis
  - perform an information technology vulnerability analysis
  - consider serious natural and societal anomalies, events or hazards that may impact information technology infrastructure

- analyze the business impacts that serious high probability natural and societal anomalies, events or hazards could have

8. Establish an information technology mitigation strategy that supports the continuity of essential business services

- ✓ Develop and implement a strategy to mitigate anomalies, events or hazards

- ✓ Base strategy on:
  - hazard analysis, internal and external hazards
  - information technology impact analysis
  - information technology risk assessment
  - information technology cost-benefit analysis
  - information technology program assessment and risks associated
  - operational experience

- ✓ Ensure information technology mitigation strategy is comprehensive and effective
  - consider neutralizing anomalies, events or hazards
  - change the nature of anomalies, events or hazards to reduce threat
  - control rate of release of the threat
  - identify information technology preventive controls
  - segregate anomalies, events or hazards from people and property
  - use building construction standards to mitigate information technology critical infrastructure
  - protect information technology critical infrastructure, resources and data from exposure
  - use protective technologies to minimize exposure
  - use communication systems to warn of impeding anomalies, events or hazards including viral attacks
  - have duplicate or redundant information technology critical infrastructure, resources and data

9. Develop an information technology business continuity resource management capability to support the continuity of essential business services

- ✓ Define information technology business continuity program resource objectives
  - ensure objectives are consistent with program goals, objectives and scope

- ✓ Set information technology business continuity objectives that address resource needs
  - availability and use of resources

- ✓ Identify information technology business continuity program resource deficiencies
  - perform an assessment that identifies program resource gaps and shortfalls
  - describe the steps that should be taken to address these gaps and shortfalls

- ✓ Maintain an inventory of information technology business continuity program resources
  - internal and external resources

10. Establish service level agreements (SLAs) to support information technology business continuity issues that support essential business services

- ✓ Negotiate information technology SLAs
  - perform needs assessment
  - develop agreements with organizations, local jurisdictions, and companies

- ✓ Ensure that information technology business continuity plans mention the agreements

11. Prepare information technology business continuity program processes and plans to support the continuity of essential business services

- ✓ Develop information technology business continuity program processes and plans
  - develop information technology mitigation, information technology contingency, information technology response, information technology recovery, information technology resumption and information technology training processes and plans

- ✓ Include common information technology processes and planning elements
  - roles and responsibilities
  - lines of authority

- ✓ Create information technology contingency plans
  - identify specific natural and societal anomalies, events or hazards

- define information technology operations, information technology organization structure per the incident command system
- define information technology resource identification, coordination, and allocation
- define information technology teams and their roles and responsibilities
- define information technology standard operating guidelines for teams and their roles
- define information technology administration processes per the incident command system
- validate the information technology contingency plan

✓ Create information technology response and crisis plans
- define information technology guidelines for activation
- define information technology organization and emergency communications
- create information technology operational impact assessments
- define the information technology general plan including associated work meetings
- define the various information technology briefings as designated in the incident command system
- create information technology initial damage assessments

✓ Create information technology recovery plans
- define information technology processes and prioritize
- identify software backups and their respective sites
- identify the removal of critical applications and or functions and systems
- create information technology salvage plans for all applicable infrastructure
  - computer equipment
  - technology facilities
- create information technology restoration plans for all applicable infrastructure
  - computer equipment
  - technology facilities

✓ Create information technology resumption plans
- operational, performance monitoring and feedback

12. Develop an event or incident coordination and control capability to support the continuity of essential business services

✓ Develop a information technology response and recovery capability

- develop the capability to manage response and recovery activities

✓ Develop an information technology incident management system
- specify who should be responsible for each incident management function

✓ Control the information technology incident management system
- discuss the incident management system with all organizations and authorities to ensure seamless operational response and recovery

✓ Create coordinating information technology policies and procedures
- establish information technology policies and procedures to coordinate with other relevant organizations, authorities and resource personnel
  - information technology response and recovery activities
  - information technology continuity of maintenance activities

13. Establish an information technology communications capability to support the continuity of essential business services

✓ Create an information technology communications capability
- establish communications systems and procedures to support program activities

✓ Create an information technology emergency alert and or warning capability
- develop an information technology system to warn people (end users) and communicate with them (e.g. viral attacks)
- test and use the information technology alert and warning systems

✓ Identify an information technology operational communications capability
- identify information technology operational communications needs
- develop information technology operational communications systems

14. Establish information technology event or incident operational procedures to support continuity of essential business services

✓ Create information technology procedures to support the program

- develop, coordinate and implement procedures to support operations

✓ Procedures to protect people, property, and the environment
- ensure that health and safety of information technology personnel are paramount
- address the need of protecting public property as pertains to information technology

✓ Develop procedures to deal with anomalies, events or hazards
- develop information technology response and recovery procedures

✓ Analyze hazardous situations that impact information technology
- assess damage caused by anomalies, hazardous events and incidents
- identify information technology resource(s) needed to recover

✓ Support information technology mitigation and recovery efforts
- ensure information technology procedures support mitigation and recovery while information technology response activities are being carried out

✓ Formulate information technology succession procedures
- ensure procedures address the need that information technology management personnel will be available to maintain functions during an event or incident
- ensure information technology procedures address the need that organizations will be available to maintain services during an event or incident

15. Establish an information technology logistical capability to support the continuity of essential business services

✓ Establish information technology logistical support
- capabilities and procedures to support the operation of the program or activity

✓ Specify successor and alternate staffs as necessary to support business continuity activities such that:
- staff be comprised of designated information technology personnel, able to execute tasks necessary to remediate, transition or relocate information technology operations from a primary to an alternate site.
- information technology successors and alternates designated to replace identified key personnel

- conditions of replacement and responsibilities, and management delegated to successors shown in the information technology plan of each organization
- instructions for information technology staff including staff assignments, alternate duty assignments, skill roster, notification procedures, and other applicable actions to be taken

✓ Establish information technology support facilities (when applicable)
- establish a primary information technology facility (for operations)
- establish an alternative facility (hot or warm site, or other)
- test information technology support facilities on an annual basis

16. Provide information technology business continuity education and training to support continuity of essential business services

✓ Create a information technology business continuity curriculum to support the program
- develop a curriculum that meets the needs
- implement the training and education curriculum

✓ Achieve information technology business continuity educational objectives
- make personnel aware of the program
- enhance the skills needed to support the program

✓ Define extent of the information technology business continuity training activities
- identify the scope of the training activities
- specify how often personnel should receive training

✓ Discuss the incident management system in relation to information technology business continuity
- teach people how to use the incident management system

✓ Maintain a record of information technology business continuity training activities
- maintain a record that documents the training and education activities and results

17. Improve the information technology business continuity program to support continuity of essential business services

✓ Evaluate the information technology business continuity program plans, procedures, capabilities

- ✓ Carry out information technology business continuity exercises to test program elements and plans

- ✓ Take corrective actions
  - o establish and apply corrective action procedures

- ✓ Update information technology business continuity plans and procedures on an annual basis to account for local, state, or federal policy or guideline changes.

18. Develop information technology business continuity financial management procedures to support continuity of essential business services

- ✓ Develop financial and administrative procedures to support information technology business continuity program operations

- ✓ Develop financial decision making procedures
  - o develop procedures that control how financial program decisions are made, authorized, expedited, decisions in compliance with accounting principles, and that support administration

Source:

- King County Information Technology Business Continuity Policy, draft 2004
- Interim Guidance on Continuity of Operations Planning for State and Local Governments, FEMA May 2004
- Standard on Disaster/Emergency Management and Business Continuity Programs, NFPA 1600 2004 Edition
- National Incident Management System, DHS March 1, 2004
- Overview of Non-Federal Partners on the National Infrastructure Protection Plan, DHS May 21, 2004 Draft
- Continuity of Operations, Government Accounting Office (GAO) February 2004 (GAO-04-160)
- Security of Federal Automated Information Resources, Office of Management and Budget Circular A-130, Appendix III, February 1996
- Contingency Planning Guide for Information Technology Systems, National Institute of Standards and Technology (NIST) 800-34
- See the King County Business Continuity Program website for links to the full list of documents: http://kcweb.metrokc.gov/oirm/projects/bc.htm